IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

CUPP CYBERSECURITY LLC et al.,	§	
	§	FILED UNDER SEAL
Plaintiffs,	§	
	§	
v.	§	Civil Action No. 3:18-cv-01251-M
	§	(Consolidated with
TREND MICRO INC., et al.,	§	Civil Action No. 3:20-cv-03206-M)
	§	
Defendants.	§	
	§	

MEMORANDUM OPINION AND ORDER

Before the Court is the Motion for Summary Judgment (ECF No. 228), filed by Defendants Trend Micro, Inc., Trend Micro America, Inc., and Trend Micro Incorporated (collectively, "Trend Micro" or "Defendants"), and the Motion for Partial Summary Judgment (ECF No. 238), filed by Plaintiffs CUPP Cybersecurity, LLC, and CUPP Computing AS (collectively, "CUPP" or "Plaintiffs"). Also pending before the Court is Trend Micro's Motion to Partially Stay the Case as to U.S. Patent Nos. 8,365,272 and 9,756,079 (ECF No. 320) and Trend Micro's Motion to Strike Portions of Dr. Cole's Opening Expert Report (ECF No. 224).

On November 10, 2022, the Court heard oral argument on the Motions. *See* ECF No. 327 ("Hearing Tr."). As stated on the record during the hearing, the Motion to Partially Stay the Case is **GRANTED**. The case is stayed as to all asserted claims of the '272 and '079 patents. In addition, as stated on the record, Trend Micro's Motion to Strike Portions of Dr. Cole's Opening Expert Report is **GRANTED.**

For the following reasons, Trend Micro's Motion for Summary Judgment is **GRANTED IN PART** and **DENIED IN PART**, and CUPP's Motion for Partial Summary Judgment is **DENIED.**

Although this Opinion may not contain any confidential information, the Court will, out of an abundance of caution, conditionally enter it under seal because the underlying motions and related documents, discussed below, were filed under seal. By **January 27, 2023,** the parties are **ORDERED** to file a joint status report that states whether any party believes this Opinion contains any confidential information that should remain sealed and, if so, attaches for the Court's consideration a proposed redacted public version of the Opinion.

I. Background

In May 2018, CUPP sued Trend Micro, asserting eight patents.[1] *See CUPP Cybersecurity LLC v. Trend Micro Inc.*, Case No. 3:18-cv-01251-M, ECF No. 1 (N.D. Tex. May 15, 2018) ("*CUPP1*"). In 2019, the case was stayed pending resolution of seven petitions for *inter partes* review ("IPR"). ECF No. 70. The stay was lifted in October 2020. ECF No. 73. The Patent Trial and Appeal Board ("PTAB") invalidated four of the asserted patents,[2] but held that the challenged claims of the '272 and '079 patents were valid. Trend Micro appealed to the Federal Circuit.

After the stay, four patents remained in *CUPP1*: the '079 patent, the '444 patent, the '272 patent, and the '202 patent. CUPP moved to amend its infringement contentions to add eight additional claims. ECF No. 79. On January 12, 2021, the Court granted CUPP's requested leave in part, holding that CUPP was allowed to amend its infringement contentions to assert only "claims 1 and 21 of the '202 patent against OfficeScan 10.6." ECF No. 87.

[1] United States Patent No. 9,756,079 ("the '079 patent"); U.S. Patent No. 9,747,444 ("the '444 patent"); U.S. Patent No. 8,365,272 ("the '272 patent"); U.S. Patent No. 8,789,202 ("the '202 patent"); U.S. Patent No. 8,631,488 ("the '488 patent"); U.S. Patent No. 9,106,683 ("the '683 patent"); U.S. Patent No. 9,843,595 ("the '595 patent"); and U.S. Patent No. 9,781,164 ("the '164 patent").

[2] The PTAB invalidated United States Patent Nos. 8,631,488 ("the '488 patent"), 9,106,683 ("the '683 patent"), 9,843,595 ("the '595 patent"), and 9,781,164 ("the '164 patent").

In October 2020, around the same time the stay was lifted in *CUPP1*, CUPP filed a second suit against Trend Micro, asserting nine patents.[3] *See CUPP Cybersecurity LLC v. Trend Micro Inc*., Case No. 3:20-cv-03206-M, ECF No. 1 (N.D. Tex. Oct. 20, 2020) ("*CUPP2*"). On November 1, 2021, *CUPP1* was consolidated with *CUPP2*. ECF No. 141.

On October 24, 2022, the Federal Circuit issued its decision on Trend Micro's appeal of the PTAB's decision upholding the validity of the '272 and '079 patents. *See* ECF No. 319. The PTAB had previously held that the asserted claims in these patents were not invalid; the Federal Circuit vacated that decision and remanded for further proceedings. Trend Micro moved to stay this case as to the '272 and '079 patents until the PTAB proceedings are completed, which the Court has granted.

a. Asserted Claims

On July 15, 2022, CUPP filed its election of asserted claims, asserting ten claims from eight patents. ECF No. 202. The asserted patents consist of four *CUPP1* patents ('079, '272, '202, '400 patents) and four *CUPP2* patents ('834, '444, '462, and '421 patents).

Of the eight asserted patents, several are related and share the same specification. For purposes of the pending summary judgment motions, the Court will provide an overview of the '202 and '400 patents (referred to as the "removable device" patents), the '444, '462, and '421 patents (referred to as the "network security" patents), and the '834 patent (referred to as the "integrity level" patent).

i. Removable Device Patents ('202 and '400 patents)

[3] U.S. Patent No. 10,417,400 (the "'400 patent"); U.S. Patent No. 10,089,462 (the "'462 patent"); U.S. Patent No. 10,417,421 (the "'421 patent"); U.S. Patent No. 10,621,344 (the "'344 patent"); U.S. Patent No. 10,291,656 (the "'656 patent"); U.S. Patent No. 10,666,688 (the "'688 patent"); U.S. Patent No. 10,162,975 (the "'975 patent"); U.S. Patent No. 10,496,834 (the "'834 patent"); U.S. Patent No. 10,951,632 (the "'632 patent")

CUPP asserts claims 11 and 21 of the ’202 patent, and claim 17 of the ’400 patent. The ’202 and ’400 patent are related and share a common specification. Both patents are directed to data and device security in the context of removable media devices, and explain that, in the prior art, “when a host device is connected to an external device such as a USB flash drive, iPod, external hard drive, etc., both devices are vulnerable to receipt of malicious code or transfer of private data.” *E.g.*, ’202 patent, at 2:22–25. The specification describes embodiments of the disclosed invention that overcome these limitations of the prior art, including, for example, a method comprising detecting a removable media device coupled to a digital device, authenticating a password to access the removable media device, injecting redirection code into the digital device, intercepting, with the redirection code, a request for data, determining to allow the request for data based on a security policy, and providing the data based on the determination. *Id.* at 2:4–52. Claim 11 of the ’202 patent claims:

> A removable media device comprising:
>
> > a login engine configured to detect coupling to a digital device, the login engine further configured to inject redirection code into the digital device after detecting the coupling to the digital device, the redirection code being configured to intercept a first function call and configured to execute a second function call in place of the first function call;
> >
> > memory comprising data; and
> >
> > a controller configured to intercept a request for the data, determine whether to allow the request for the data based on a security policy, the security policy implementing content analysis and risk assessment algorithms, and provide requested data based on the determination.

’202 patent, cl.11.

This Court previously construed “a removable media device comprising:” in claim 11 of the ’202 patent to be limiting. ECF No. 150 at 11.

Claim 21 of the ’202 patent claims:

> A non-transitory computer readable storage media comprising instructions, the instructions executable by a processor to perform a method, the method comprising:
>
> > detecting a removable media device coupled to a digital device;
> >
> > injecting redirection code into the digital device after detecting the removable media device is coupled to the digital device, the redirection code configured to intercept a first function call and configured to execute a second function call in place of the first function call;
> >
> > intercepting, with the redirection code, a request for data on the removable media device;
> >
> > determining whether to allow the intercepted request for data based on a security policy, the security policy implementing content analysis and risk assessment algorithms; and
> >
> > providing requested data based on the determination.

Id. cl.21.

This Court previously construed "injecting redirection code into the digital device" in claim 21 of the '202 patent to mean "the redirection code is injected from outside the digital device into the digital device." *Id.* at 32. The Court also construed "a request for the data" and "a request for data on the removable media device," as those terms appear in claims 11 and 21 of the '202 patent, to have their plain and ordinary meaning. *Id.* at 34–35.

Claim 17 of the '400 patent recites:

> A non-transitory computer readable media comprising instructions, the instructions executable by a processor to perform a method, the method comprising:
>
> > detecting a removable media device being coupled to an external device port of a digital device, the digital device having an operating system and a file system, the removable media device having a login module;
> >
> > causing, after detecting the removable media device being coupled to the external device port of the digital device, at least a portion of redirection code to be generated on the digital device by the login module of the removable media device, the redirection code including an interceptor, a data security policy, and a data security process;
> >
> > intercepting, using the interceptor, a first function call to the operating system or the file system of the digital device before the first function call is executed

> by the operating system or the file system, the first function call including a request of the operating system or the file system to retrieve data from or write data to the removable media device, the first function call being initiated by a particular user or a particular application; and
>
> performing a set of one or more second function calls in response to intercepting the first function call, the set of one or more second function calls not including the first function call, the set of one or more second function calls including a data-security-based second function call, the data-security-based second function call causing the steps of:
>
>> executing the data security process, the data security process determining whether the particular user or the particular application is authorized to retrieve the data from or write the data to the removable media device, and thus whether to allow the first function call based at least on results of the data security process; and
>>
>> allowing the operating system or the file system to execute the first function call in response to a determination to allow the first function call.

’400 patent, cl.17.

ii. Network Security Patents (’444, ’462, and ’421 patents)

CUPP asserts claims 11 and 21 of the ’444 patent, claim 11 of the ’462 patent, and claim 1 of the ’421 patent. The ’444 patent is the parent of the ’462 and ’421 patents, and the three patents share the same specification. These network security patents describe protecting mobile devices against attacks and malicious code. *See, e.g.*, ’444 patent, Abstract; *id.* at 2:41–49. The specification describes a security system that employs security policies for determining whether a mobile device is in a trusted network, and whether to allow network data to be forwarded to the mobile device. *Id.* at 3:26–58. Claim 11 of the ’444 patent recites:

> A method comprising:
>
> storing in security system memory a security policy identifying one or more trusted networks and defining when to forward network data intended for a mobile device to the mobile device for processing by at least one mobile device processor of the mobile device, the at least one mobile device processor of the mobile device being different than a security system processor of the security system,
>
>> the security policy defining that when the mobile device does not reside on any of the one or more trusted networks identified by the security policy, the

> > security system processor of the security system will scan the network data for malicious content to decide whether the network data should be forwarded to the mobile device,
> >
> > the security policy defining that when the mobile device resides on any of the one or more trusted networks identified by the security policy, the security system processor of the security system will allow the network data to be forwarded to the mobile device without the security system processor of the security system scanning for the malicious content;
>
> receiving from the mobile device particular network data before the at least one mobile device processor of the mobile device processes the particular network data, the particular network data having been forwarded to the security system by the at least one mobile device processor of the mobile device; and
>
> executing security code to implement the security policy as it relates to the particular network data received from the mobile device, the executing the security code including modifying at least a portion of the particular network data before delivering the particular network data as modified to the mobile device.

Id. cl.11.

Claim 21 of the ’444 patent recites:

> A security system comprising:
>
> > security system memory storing a security policy identifying one or more trusted networks and defining when to forward network data intended for a mobile device to the mobile device for processing by at least one mobile device processor of the mobile device, the at least one mobile device processor of the mobile device being different than a security system processor of the security system,
> >
> > > the security policy defining that when the mobile device does not reside on any of the one or more trusted networks identified by the security policy, the security system processor of the security system will scan the network data for malicious content to decide whether the network data should be forwarded to the mobile device,
> > >
> > > the security policy defining that when the mobile device resides on any of the one or more trusted networks identified by the security policy, the security system processor of the security system will allow the network data to be forwarded to the mobile device without the security system processor of the security system scanning for the malicious content;
> >
> > means for receiving from the mobile device particular network data before the at least one mobile device processor of the mobile device processes the particular network data, the particular network data having been forwarded to

> the security system by the at least one mobile device processor of the mobile device; and
>
> security code configured to implement the security policy as it relates to the particular network data received from the mobile device, the security code configured to modify at least a portion of the particular network data before delivering the particular network data as modified to the mobile device.

Id. cl.21.

Relevant here, the Court construed "means for receiving from the mobile device particular network data before the at least one mobile device processor of the mobile device processes the particular network data, the particular network data having been forwarded to the security system by the at least one mobile device processor of the mobile device" in claim 21 of the '444 patent as a means plus function claim, in which the function is "receiving from the mobile device particular network data before the at least one mobile device processor of the mobile device processes the particular network data, the particular network data having been forwarded to the security system by the at least one mobile device processor of the mobile device," and the associated structure is connection mechanisms for USB, Ethernet, WiFi, WiMAX, GSM, CDMA, BlueTooth, PCMCIA, modem, or NIC. ECF No. 150 at 18.

Claim 11 of the '462 patent recites:

> A security method, comprising:
>
> determining whether a mobile device is on any of one or more trusted networks by searching for a predetermined network device on the one or more trusted networks;
>
> disabling all data transfer via resident devices resident on the mobile device, when the mobile device is outside of any of the one or more trusted networks and when a trusted security device is not coupled to a mobile device data port of the mobile device, the mobile device including at least one mobile device processor, mobile device memory and the mobile device data port, the mobile device memory having data transfer code and a data transfer policy thereon, the data transfer policy including information for identifying the one or more trusted networks;

> enabling data transfer via at least one of the resident devices resident on the mobile device, when the mobile device is outside of any of the one or more trusted networks and only if the trusted security device is coupled to the mobile device data port of the mobile device;
>
> enabling a trusted information technology (IT) person of a trusted enterprise to activate and deactivate at least a portion of the data transfer code;
>
> receiving particular incoming data by a particular trusted security device before the at least one mobile device processor processes the particular incoming data, the particular trusted security device including at least one security device processor, security device memory and a security device data port, the security device data port configured to couple to the mobile device data port, the at least one security device processor being different than the at least one mobile device processor, the security device memory including security code and a security policy thereon; and using the security code to evaluate the particular incoming data for malware to implement the security policy as it relates to the particular incoming data.

’462 patent, cl.11.

Claim 1 of the ’421 patent recites:

A system, comprising:

> a mobile device including at least one mobile device processor, mobile device memory and a mobile device data port, the mobile device memory having data transfer code and a data transfer policy thereon,
>
> > the data transfer code being configured to disable all data transfer via resident devices resident on the mobile device, when the mobile device is outside of any of one or more trusted networks and when a trusted security device is not coupled to the mobile device data port of the mobile device,
> >
> > the data transfer code being configured to determine whether the mobile device is on any of the one or more trusted networks by searching for a predetermined network device on the one or more trusted networks,
> >
> > the data transfer code being configured to enable data transfer via at least one of the resident devices, when the mobile device is outside of any of the one or more trusted networks and only if the trusted security device is coupled to the mobile device data port of the mobile device,
> >
> > the data transfer policy including information for identifying the one or more trusted networks, and

> > the mobile device including a redirector executable by the at least one mobile device processor to redirect particular incoming data from the mobile device to a particular trusted security device; and
>
> the particular trusted security device including at least one security device processor, security device memory and a security device data port, the security device data port configured to couple to the mobile device data port, the at least one security device processor being different than the at least one mobile device processor, the security device memory including security code and a security policy thereon,
>
> > the security code configured to receive the particular incoming data before the at least one mobile device processor processes the particular incoming data,
> >
> > the security code configured to evaluate the particular incoming data for malware to implement the security policy as it relates to the particular incoming data; and
> >
> > the security code configured to prevent at least a portion of the particular incoming data from being processed by the at least one mobile device processor or configured to modify at least a portion of the particular incoming data before being processed by the at least one mobile device processor.

’421 patent, cl.1.

iii. Integrity Level Patent (’834 patent)

CUPP asserts claim 1 of the ’834 patent. The ’834 patent is titled “Secure computing system,” and is directed towards a computer system with multiple security levels based, in part, on independent “security aspects,” which include confidentiality and integrity. ’834 patent, at 1:64–3:4. The computer system described by the ’834 patent has multiple security levels, comprising high-power and low-power processing devices, and an interface unit comprising functions for moving classified information between the devices according to formal rules governing the security aspects of confidentiality and/or integrity. *Id.* at 6:35–42. Claim 1 of the ’834 patent recites:

> A system comprising:

> a virtual machine engine for generating one or more virtual machines, each virtual machine being generated having a virtual machine confidentiality level and a virtual machine integrity level, the virtual machine confidentiality level being selected from at least a higher confidentiality level and a lower confidentiality level, the virtual machine integrity level being selected from at least a higher integrity level and a lower integrity level, a first virtual machine with the higher confidentiality level being configured to require a stronger confidentiality process than a second virtual machine with the lower confidentiality level, a third virtual machine with the higher integrity level being configured to require a stronger integrity process than a fourth virtual machine with the lower integrity level;
>
> a first program;
>
> a second program;
>
> a first datastore or data set associated with a first data confidentiality level and a first data integrity level;
>
> a second datastore or data set associated with a second data confidentiality level and a second data integrity level;
>
> at least one hardware processor configured to:
>
>> receive a request to use the first program;
>>
>> execute a particular virtual machine with a particular virtual machine confidentiality level and a particular virtual machine integrity level;
>>
>> use a particular confidentiality process and a particular integrity process before or while operating the first program by the particular virtual machine, the particular confidentiality process being associated with the particular virtual machine confidentiality level, the particular integrity process being associated with the particular virtual machine integrity level;
>>
>> allow the first program to read the first data set or from the first datastore, only if the first data confidentiality level of the first data set or the first datastore is equal to or lower than the particular virtual machine confidentiality level, and only if the first data integrity level of the first data set or the first datastore is equal to or higher than the particular virtual machine integrity level.

Id. cl.1.

The Court previously construed “integrity level” to mean “a security aspect, separate from the confidentiality level, that indicates reliability.” ECF No. 151 at 23.

b. Accused Products

Trend Micro sells a variety of computer security products, which bundle together various features or employ various services that implicate the asserted patents. The Court will provide a brief overview of the accused products as they are relevant to the summary judgment motions.

Trend Micro Mobile Security for Enterprise ("Mobile Security") is a Trend Micro product that allows a company to add security to employee's phones, including the ability to remotely lock or wipe the phones. The company uses the "Management Server" software at the company's premises, and employees install the "Mobile Security" app on their phone. Mobile Security is used in conjunction with other Trend Micro services, including the "Mobile App Reputation Service" ("MARS") and "Web Reputation Service" ("WRS").

Trend Micro also produces computer security software, which it sells under a variety of different names, including OfficeScan, Apex One, and the Worry-Free Products. These software products generally provide security for Windows computers, including anti-malware software that can scan a computer for malware or viruses. Relevant here, these products contain "Data Loss Prevention" and "Device Control" features, referred to as "DLP" and "DC" features, respectively. The DLP feature prevents against accidental or deliberate leakage of sensitive data, including by blocking emails that include sensitive information like credit cards or social security numbers, or preventing the computer from saving files on a USB flash drive device. The DC feature regulates a computer's access to external storage devices and network devices. For example, DC could permit a computer to read from a USB device connected to the computer, but prevent the computer from saving files (or "writing") to the USB device.

Finally, Trend Micro produces and sells the Trend Micro Portable Security product, which is a portable USB device that includes a virus-scanning program. Customers can take the USB from computer to computer and scan each computer for viruses.

Trend Micro has, at times, sold collections of its products as "Smart Protection Suites"; these suites are collections of other products, and include both accused and unaccused products. No additional functionality in these suites is provided beyond the functionality in the underlying products.

II. Legal Standard

Summary judgment is proper when there is no genuine issue as to any material fact and the movant is entitled to judgment as a matter of law. Fed. R. Civ. P. 56(a). Once the movant shows that there is no genuine issue as to any material fact, the burden shifts to the nonmoving party to produce competent evidence showing the existence of a genuine issue as to a material fact. *Celotex Corp. v. Catrett*, 477 U.S. 317, 330 (1986). The Court views all evidence in the light most favorable to the party opposing the motion. *Applied Med. Res. Corp. v. U.S. Surgical Corp.*, 448 F.3d 1324, 1331 (Fed. Cir. 2006).

III. Trend Micro's Motion for Summary Judgment

Trend Micro moves for summary judgment of noninfringement for the asserted claims of the '400, '202, '444, '421, and '462 patents.[4] Trend Micro also seeks summary judgment of invalidity as to claim 11 of the '202 patent for lack of written description, summary judgment of no pre-suit indirect or willful infringement, and additionally, summary judgment of no indirect infringement under CUPP's theory that Trend Micro's customers infringe the asserted patents.

[4] Trend Micro also moves for summary judgment of non-infringement of claim 7 of the '079 patent and claim 16 of the '272 patent. However, because the Court has stayed the case as to the '079 and '272 patents, it does not reach those arguments.

a. Non-infringement of claim 17 of the ’400 patent

Trend Micro seeks summary judgment of non-infringement of claim 17 of the ’400 patent by all asserted products containing the “Data Loss Prevention” and “Device Control” features, which the parties generally refer to as the “DLP/DC” products.[5] The parties agree that the DLP/DC products consist of software installed on a digital device, such as a computer. Hearing Tr. at 4–5, 21. Claim 17 of the ’400 patent describes instructions that cause a processor to perform a method, which includes, in part, “causing, after detecting the removable media device being coupled to the external device port of the digital device, at least a portion of redirection code to be generated on the digital device by the login module of the removable media device.” ‘400 patent, cl. 17 (emphasis added).

Trend Micro contends that CUPP’s infringement expert, Dr. Cole, has not set forth a viable theory for how the DLP/DC products satisfy the “removable media device” or “causing . . . redirection code to be generated” limitations. Specifically, because the DLP/DC products are undisputedly software, Trend Micro contends that they categorically cannot perform any limitation that requires action by the removable media device, namely, they cannot generate code by the login module of the removable media device. Put differently, Trend Micro argues that CUPP does not identify any “removable media device” that is part of the DLP/DC products that satisfies this disputed claim element.

In response, CUPP argues that Trend Micro disregards claim language requiring “causing, *after detecting the removable media device being coupled to the external port of the digital device*” at least a portion of redirection code to be generated. According to CUPP, the DLP/DC products satisfy this limitation because after a USB drive is inserted into a digital

[5] These products include the Apex One, OfficeScan, Worry Free, and Smart Protection products. ECF No. 229-1 at 18.

device, the DLP/DC products respond by performing "Autorun prevention" capability to prevent the contents of the USB drive from automatically running on the digital device, which generates redirection code to redirect potentially harmful actions by Autorun-based malware from the USB drive. *See* ECF No. 271-2 at 9 ("Once detected, the smart Autorun prevention capability causes the DC/DLP products to generate redirection code on the computer, including by adding or updating information for the data security policies regarding the removable device or the content within the device."). In other words, insertion of a USB device is detected, then the DLP/DC product causes an Autorun prevention program to run, which generates redirection code on the computer.

As an initial matter, the Court notes that the parties do not appear to dispute how the DLP/DC products function for purposes of this claim limitation; instead, the issue is one of claim interpretation, namely whether the claim language permits a module on the digital device to cause the redirection code to be generated, as opposed to something on the removable media device.

The Court concludes that the claim language is clear, and requires that the causing of the redirection code being generated on the digital device is "the login module of the removable media device." In other words, the login module of the removable media device is the component that causes the redirection code to be generated. By relying on Autorun prevention software in DLP/DC products that are installed on the digital device, CUPP's infringement theory improperly disregards the requirement that the login module be located on the removable media device. *See MicroStrategy Inc. v. Bus. Objects, S.A.*, 429 F.3d 1344, 1352 (Fed. Cir. 2005) ("If . . . even one claim limitation is missing or not met, there is no literal infringement.").

Nor does the Court find that the "after detecting . . ." clause relied on by CUPP warrants a different conclusion. This limitation simply provides a temporal component as to when the login module of the removable media device causes redirection code to be generated, *i.e.*, after the coupling of a removable media device to the digital device. It does not render meaningless the other limitations in claim 17, including the limitation that redirection code is generated on the digital device by the login module of the removable media device.

Because there is no factual dispute for the jury to resolve, the Court concludes, as a matter of law, that the accused DLP/DC products do not infringe claim 17 of the '400 patent. Trend Micro is entitled to summary judgment on this claim.

b. Non-infringement of claim 21 of the '202 patent

Trend Micro seeks summary judgment of non-infringement of claim 21 of the '202 patent by all accused products. The Court previously granted Trend Micro's Motion to Strike Portions of Dr. Cole's Opening Expert Report, the result of which means that CUPP is limited to accusing only OfficeScan 10.6 of infringing claim 21 of the '202 patent. OfficeScan 10.6 falls in the DLP/DC category of accused products, which the parties agree consist of software loaded onto a "digital device," such as a laptop or desktop computer.

Claim 21 of the '202 patent is a method claim, and as construed by the Court, requires "injecting redirection code" from outside the digital device into the digital device. Trend Micro argues that summary judgment of non-infringement is appropriate because CUPP's infringement expert for the '202 patent, Dr. Cole, provides no explanation for how the accused products satisfy this "injecting" limitation. Because it is undisputed that the accused products exist on the digital device, Trend Micro argues there is no evidence that the accused products perform the claimed method step of injecting redirection code from outside the digital device into the digital device.

In its response brief, CUPP argues that the DLP/DC and OfficeScan products use an outside server to inject redirection code into a client program running on a digital device after detecting a removable device coupled to the digital device; put differently, an external server—referred to as the OfficeScan or Apex One server—sends the redirection code to the digital devices where the DLP/DC products are installed. In reply, Trend Micro argues that this "server" argument is not in Dr. Cole's infringement report, and thus was never disclosed and is inadmissible.

Dr. Cole's infringement report is 2,345 pages long. *See* Def. App. 254–2597 (ECF No. 229) ("Cole Rep."). At ¶ 2020 of his report, Dr. Cole begins discussing the "injecting" limitation in claim 21 of the '202 patent—identified in his report as element 21(c)—for various Trend Micro products. Paragraphs 2059 through 2144 of his report discuss the "injecting" limitation for the DLP/DC products specifically, which include OfficeScan. Cole Rep. ¶¶ 2059–2144.

The Court has reviewed these paragraphs and agrees with Trend Micro that Dr. Cole does not describe a server as the source of redirection code being injected from outside a digital device into the digital device. There is no discussion of an OfficeScan or Apex One server, let alone a server that "injects" code into a digital device. While the word "server" appears several times throughout these paragraphs, it appears almost exclusively as part of various directory paths identifying source code files, and not in textual sentences. Put differently, there is no identification or discussion of any server in or associated with the DLP/DC products in connection with the "injecting" limitation of claim 21. As a result, the portions of Dr. Cole's report discussing infringement by the DLP/DC products of the "injecting limitation" in claim 21 of the ’202 patent do not disclose using the OfficeScan server to inject code into the digital device to satisfy this limitation. *See Intell. Sci. & Tech., Inc. v. Sony Elecs., Inc.*, 589 F.3d 1179, 1183 (Fed. Cir. 2009) (“[A] patentee’s expert must set forth the factual foundation for his infringement opinion in sufficient detail for the court to be certain that features of the accused product would support a finding of infringement . . . .”).

In addition, the Court has reviewed the paragraphs of Dr. Cole’s report cited by CUPP in support of this issue in CUPP’s responsive brief, and concludes that none of them connect an OfficeScan server with claim 21 of the ’202 patent in a way that could be deemed a disclosure of the theory of infringement now argued by CUPP. *See* ECF No. 271-2 at 11–14 (citing Cole Rep. ¶¶ 96, 126–131, 143, 944, 2069, 2071, 2075–2135).[6] During the hearing, the Court asked CUPP to point it to the specific paragraphs in Dr. Cole’s report that it contends disclose its server theory, and again CUPP referenced paragraphs that the Court has determined do not provide adequate disclosure. Hearing Tr. at 106–09 (citing Cole Rep. ¶¶ 96, 143, 2062–63, 2069, 2072, 2080–82). To the extent other unidentified portions of Dr. Cole’s report may discuss CUPP’s server theory, that evidence is not properly before the Court. *See Malacara v. Garber*, 353 F.3d 393, 405 (5th Cir. 2003) (“When evidence exists in the summary judgment record but the nonmovant fails even to refer to it in the response to the motion for summary judgment, that evidence is not properly before the district court.”); *Ragas v. Tenn. Gas Pipeline Co.*, 136 F.3d 455, 458 (5th Cir. 1998) (“The party opposing summary judgment is required to identify specific evidence in the record and to articulate the precise manner in which that evidence supports his or

[6] As discussed, the Court has already reviewed ¶¶ 2059–2144 of Dr. Cole’s report and found no disclosure of the server theory CUPP now urges. The remaining paragraphs similarly do not disclose this theory of infringement, and instead discuss general background of the accused products or infringement theories for claims of a different patent. *See* Cole Rep. ¶ 96 (providing a general overview of the Apex One accused product), ¶¶ 126–31 (describing Dr. Cole’s testing of Trend Micro products, including Apex One, without any reference to a server), ¶ 143 (describing infringement of element 1(a) of the ’400 patent), ¶ 944 (describing DLP/DC products when describing infringement of element 17(b) of the ’400 patent).

her claim."); *cf. United States v. Dunkel*, 927 F.2d 955, 956 (7th Cir. 1991) ("Judges are not like pigs, hunting for truffles buried in briefs.").

At the hearing, CUPP argued that Dr. Cole discloses the OfficeScan server by citing Trend Micro documents, which in turn describe how certain accused products have functionality involving a server. However, such citations—which occur in ¶¶ 96 and 143, portions of Dr. Cole's report describing general background, and not his element-by-element infringement analysis of the '202 patent—are too attenuated to qualify as sufficient disclosure of CUPP's infringement theory. *E.g.*, *Intell. Sci.*, 589 F.3d at 1186 ("Asking litigants to provide more than a difficult-to-decipher expert declaration does not impose too high a burden at summary judgment . . . ."). None of the paragraphs in Dr. Cole's report pointed to by CUPP describe the server "injecting" redirection code into a digital device with any specificity that could be deemed a cogent infringement theory. Simply identifying the existence of a server, without explaining how that server satisfies the particular claim limitation, is insufficient.

The Court concludes that, because CUPP's infringement theory for claim 21 of the '202 patent based on an outside server "injecting" redirection code is not in the report of Dr. Cole, CUPP's sole infringement expert as to the '202 patent, it is not admissible and cannot create a genuine issue of material fact at trial. *See* Fed. R. Civ. P. 26(a)(2). For the same reason, CUPP cannot point to Dr. Cole's deposition testimony to support its otherwise undisclosed server theory. Federal Rule of Civil Procedure 37 provides that if a party fails to provide information as required by Rule 26(a), the party is not allowed to use that information to supply evidence on a motion, at a hearing, or at a trial, unless the failure was substantially justified or is harmless. CUPP provides no explanation for why Dr. Cole's server theory of infringement was not disclosed in his report, and accordingly, the Court will not consider Dr. Cole's deposition testimony on this issue.

For the foregoing reasons, the Court concludes that there is no genuine issue of material fact that the accused DLP/DC products do not satisfy the "injecting redirection code" limitation of claim 21 of the '202 patent. Summary judgment of non-infringement is therefore appropriate as to that claim.

The Court further finds that, without regard to the undisclosed server theory, summary judgment for Trend Micro on claim 21 of the '202 patent is appropriate for an additional reason, namely that there is unrebutted evidence that there were no infringing sales of OfficeScan 10.6—the only remaining accused product as to claim 21—during the '202 patent term. Trend Micro points to a declaration of Trend Micro manager Michael Chang, who states that on June 30, 2014, OfficeScan 10.6 was put on "End of Sale" status, which refers to "the date that Trend Micro will cease to make a product generally available for purchase or renewal." Def. App. 6064. The '202 patent issued on July 14, 2014, and accordingly, Trend Micro argues there were no infringing sales during the '202 patent term. In response, CUPP points only to documents indicating that sales of subsequent versions of OfficeScan, including OfficeScan XG, occurred during the patent term. Because there is unrebutted evidence that sales of OfficeScan 10.6 ceased in June 2014, prior to the date the '202 patent issued, summary judgment of non-infringement is appropriate on this basis as well.

c. Non-infringement based on the "before . . . processes" limitations in claims 11 and 21 of the '444 patent and claim 1 of the '421 patent

Trend Micro moves for summary judgment of non-infringement of claims 11 and 21 of the '444 patent and claim 1 of the '421 patent on the grounds that CUPP has not shown that the accused products satisfy the "processing" limitation of the claims.

Claims 11 and 21 of the ’444 patent describe a method for, or a security system having the means for, “receiving from the mobile device particular network data before the at least one mobile device processor of the mobile device processes the particular network data.” *See* ’444 patent, cls.11, 21 (emphasis added). Similarly, claim 1 of the ’421 patent recites “security code configured to receive the particular incoming data before the at least one mobile device processor processes the particular incoming data.” *See* ’421 patent, cl.1 (emphasis added). The parties agree that the language in these claims describing the security system receiving network data “before the at least one mobile device processor . . . processes the particular incoming data” should be interpreted consistently for all three claims. *See* Hearing Tr. at 10, 71. Claims 11 and 21 of the ’444 patent and claim 1 of the ’421 patent all generally describe a security system intervening to receive particular network data before the mobile device’s processor processes that particular network data.

As part of his infringement theory for these particular limitations, Dr. Mitzenmacher, CUPP’s infringement expert for the ’444, ’421, and ’462 patents, relies on the fact that mobile devices, such as cell phones, running Trend Micro Mobile Security will send network data to Trend Micro’s MARS and WRS services, which Dr. Mitzenmacher identifies as the “security system,” using the language of the claims. *E.g.*, ECF No. 229-3 at Def. App. 2599–3992(“Mitzenmacher Rep.”) ¶ 112. MARS is used with the Trend Micro Mobile Security for Enterprise Product; it consists of a server that will send out information about third-party applications and whether they are trustworthy. WRS employs a similar server, except that, upon submission of a URL, it will send out information about the trustworthiness of websites. According to CUPP, generally speaking, the security system, by way of the MARS and WRS servers, receives network data in the form of URLs and application information from the mobile device before the mobile device processor can process that data.

Trend Micro contends that summary judgment of non-infringement is appropriate, arguing that the mobile device cannot send data to the security system without necessarily processing it somehow, including by isolating the particular URL or application information from the network data generally. The parties agree that the mobile device simply forwarding data to the servers—*i.e.*, whatever data enters the mobile device is the exact same data that leaves the mobile device to go to the servers—does not constitute the mobile device processing the data. Hearing Tr. at 79–80. Instead, Trend Micro argues that because less than the entirety of network data that is received by the mobile device is subsequently sent to the security system—or, because "what's coming in the front door, so to speak, is different than what's going out the back door"—the mobile device processor necessarily processes the network data to some extent. *See id.* at 87.

For example, Dr. Mitzenmacher's report generally describes "network data" and "incoming data," as those terms appear in the asserted claims of the '444 and '421 patents, respectively, as taking the form of "files, URLs, and applications." *See, e.g.*, Mitzenmacher Rep. ¶¶ 113, 136, 189 ('444 patent); *id.* ¶ 606 ('421 patent). Dr. Mitzenmacher then describes the security service receiving "particular network data, such as application information, URLs, or file information [which] is forwarded from [the] mobile device to the security system on the server side of the accused products so that the security system provides the result of its analysis back to the mobile device." *Id.* ¶ 191; *see also id.* ¶ 605 ("The Accused Products receive from the mobile device particular network data, such as URLs, information about mobile applications (e.g., app name, version, hash of the file, etc.), among others, and provide such information to the security system for analysis and policy enforcement.”).

Trend Micro points to the fact that, under Dr. Mitzenmacher’s theory of infringement, the mobile device receives more network data than it sends to the security service; for example, the mobile device may download an application, but sends only information about the application (such as its name, version, and file hash) to the security system. Trend Micro contends that the mobile device’s processors necessarily would have to process that data at least somewhat in order to transmit it to the Trend Micro services. ECF No. 229-1 at 37. For support, Trend Micro points to an example from Dr. Mitzenmacher’s report describing how “the mobile device agent can send application information via an API query to the server which then returns a response indicating whether the application is likely malicious.” Mitzenmacher Rep. ¶ 114. Because such a query would be sent via the processor on the mobile device, Trend Micro argues that the application data is processed at least to the point to generate a query and generate descriptive information about the application, which according to Trend Micro, counts as “processing.” *See* Hearing Tr. at 87. For additional support, Trend Micro points to the specification of the network security patents, which discusses a “kernel-level architecture” that could allow for a mobile device to send network data without processing it, but Dr. Mitzenmacher does not explain how such a structure is present in MARS or WRS. *E.g.*, ’444 patent, at 14:31–36.

CUPP responds that simply sending particular data—be it a URL or application information—without actually performing any operations the data is programmed to perform does not count as “processing” the data. Specifically, CUPP contends that processing the data would involve actually accessing the website at the URL or the particular application. *See, e.g.*, Mitzenmacher Rep. ¶ 189 (“The Accused Products receive network data from the mobile device, which can be in the form of URLs, files, or applications, before the mobile device processor processes the network data so that the Accused Products can prevent execution or installation of malicious network files, URLs, or applications.").

The Court disagrees with Trend Micro, and finds that summary judgment is inappropriate here, as a reasonable factfinder could find that the MARS and WRS servers receive the network data at issue before the mobile device processes that data. As described in Dr. Mitzenmacher's report, the network data has not been processed by the mobile device when it is received by the MARS and WRS servers; it is not manipulated, executed, or permitted to run. Instead, Dr. Mitzenmacher's report describes the servers receiving particular network data, namely immutable information and characteristics about the network data itself for the security system to process and evaluate. Trend Micro has not convinced the Court that the collection of immutable information such as a URL or application name and version qualifies as "processing" that data in the context of the '444 and '421 patents. That is particularly so given that the "before . . . processes" limitations at issue appear to be directed towards the patents' goal of preventing the mobile device from accessing malicious software and URLs, and not simply ensuring that all the network data received by the mobile device is then forwarded wholesale to the security system, which is what Trend Micro would require. *E.g.*, '444 patent, Abstract ("A small piece of hardware connects to a mobile device and filters out attacks and malicious code. Using the piece of hardware, a mobile device can be protected by greater security . . . .").

Moreover, Trend Micro disregards other disclosures in Dr. Mitzenmacher's report describing different methods by which the MARS and WRS servers can receive particular network data before the mobile device processes the application, including receiving the entire application itself. *E.g.*, Mitzenmacher Rep. ¶ 604 ("The security code is configured to receive incoming data, e.g., app information, such as the app name *or the app itself*, before a mobile device is able to finish the installation of the app. For example, the MARS obtains mobile application information in a variety of ways such as sample submissions, crawlers, Trend Micro's own products, among others, which can be obtained before the mobile device processes the mobile application." (emphasis added)). Trend Micro does not address this example, in which the security code on the security device is configured to receive the application itself; here, it appears that the mobile device would simply be forwarding the data in question to the security system, which the parties have agreed does not qualify as the mobile device processing the data. Hearing Tr. at 79–80.

For the foregoing reasons, the Court declines to grant summary judgment of non-infringement on these grounds.

d. Non-infringement based on "disabling all data transfer" limitations in claim 11 of the '462 patent and claim 1 of the '421 patent

Trend Micro moves for summary judgment of non-infringement of claim 11 of the '462 patent and claim 1 of the '421 patent on the grounds that the accused Mobile Security products do not satisfy the limitations requiring "disabling all data transfer" in each respective claim.

Claim 11 of the '462 patent, a method claim, recites, in part, "disabling <u>all data transfer via resident devices resident on the mobile device</u>, when the mobile device is outside of any of the one or more trusted networks and when a trusted security device is not coupled to a mobile device data port of the mobile device." '462 patent, at 16:27–31 (emphasis added). Claim 1 of the '421 patent similarly describes a system that includes code being configured "to disable <u>all data transfer via resident devices resident on the mobile device</u>" when the mobile device is outside trusted networks. '421 patent, at 15:15–17 (emphasis added).

Trend Micro contends that summary judgment is appropriate because, for both claims, disabling "all data transfer via resident devices resident on the mobile device" requires that all modes of transferring data on the mobile device are deactivated, but CUPP discloses a theory of infringement in which not all methods of data transfer are disabled. Specifically, CUPP contends that neither asserted claim requires that all data transfer or all resident devices be disabled, and the specification similarly does not require that all types of network connections are disabled. ECF No. 271-2 at 36–38. CUPP maintains that the relevant limitations can be met by showing that only certain methods of data transfer are disabled, and to prove infringement, points to instances "where all data transfers via *exemplary* resident devices are disabled." *Id*. at 36–37 (emphasis added) (citing Mitzenmacher Rep. ¶¶ 229–30, 393, 399–407, 411–12). For example, Dr. Mitzenmacher describes how the accused Mobile Security products can disable all data transfers via Wi-Fi, and thus, "all data transfers via resident device(s) associated with Wi-Fi are disabled." *Id.* at 37 (citing Mitzenmacher Rep. ¶¶ 395, 400–01, 403–06).

Both asserted claims at issue require disabling or code that is configured to disable "all data transfer via resident devices resident on the mobile device" when two conditions are satisfied; namely, if the device is both outside of a trusted network and is not coupled to a trusted security device. Both asserted claims likewise describe subsequently enabling "data transfer via at least one of the resident devices . . . only if the trusted security device is coupled to the mobile device data port of the mobile device." '421 patent, at 15:26–32; '462 patent, at 16:38–43. Generally, therefore, both asserted claims first describe a "disabling" step where data transfer is restricted when the mobile device is in an unsafe network and not coupled to a security device, and then a subsequent "enabling" step, where data transfer is enabled for at least one resident device only if the mobile device is coupled to a trusted security device.

The parties do not present a factual dispute regarding the operation of the accused products, nor does CUPP contend that it has demonstrated that all modes of transferring data on the mobile device are disabled in the accused products. Instead, this is a legal dispute to be resolved by the Court regarding the scope of the phrase "disabling all data transfer via resident devices resident on the mobile device," as it appears in claim 11 of the '462 patent and claim 1 of the '421 patent. The instant dispute concerns the degree to which the data transfer is restricted in the disabling step; Trend Micro contends that, in the disabling step, no data transfer by any resident device is allowed, whereas CUPP contends that the limitation can be satisfied by showing that all data transferred via at least one resident device is disabled, without having to show that transfer via all resident devices is disabled.

As an initial matter, the Court notes that the term "resident device" is not defined in the claims and does not appear in the specification. Nor do the parties provide any evidence indicating that the term "resident device" is a term of art. Despite this, the parties appear to agree that "resident device," as it is used in these claims, generally refers to a means through which data is transferred. *See* ECF No. 229-1 at 39 ("'[V]ia resident devices' refers to mechanisms by which the recited data would be transferred . . . ."); ECF No. 271-2 at 37 (describing Wi-Fi and a cellular network connection as "different type[s] of connections associated with a different resident device"). Given the absence of any contrary intrinsic or extrinsic evidence to the contrary, the Court finds no reason to disagree with the parties' tacit agreement as to the meaning of "resident device."

To determine the scope of disabling "all data transfer via resident devices resident on the mobile device," the Court looks to the plain meaning of the claim terms, read in the context of the patents as a whole. *See Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005) (en banc) ("[T]he person of ordinary skill in the art is deemed to read the claim term not only in the context of the particular claim in which the disputed term appears, but in the context of the entire patent, including the specification."); *ACTV, Inc. v. Walt Disney Co.*, 346 F.3d 1082, 1088 (Fed. Cir. 2003) ("While certain terms may be at the center of the claim construction debate, the context of the surrounding words of the claim also must be considered in determining the ordinary and customary meaning of those claims.").

In doing so, the Court concludes that Trend Micro's interpretation is more persuasive. The claims require disabling all data transfer "via resident devices"—*i.e.*, by the means by which data can be transferred—that are "resident on the mobile device." Put differently, the resident *devices*, plural, on the mobile device—be it Wi-Fi, cellular transfer, Bluetooth, or whatever other means for transferring data that happen to be on the mobile device—must be disabled from transferring any data in order to satisfy the claim limitation. The subsequent enabling step in both claims supports the conclusion that data transfer via all the resident devices are disabled, and then "data transfer via *at least one* of the resident devices"—of the potentially multiple that are initially disabled—is later enabled after it is coupled with a trusted security device. Had the patentee intended that the disabling step could be met by disabling only certain, as opposed to all, resident devices on the mobile device, it could have said so using the same "at least one of the resident devices" language as the enabling step.

CUPP contends that the claim language "does not state disable all data transfers or disable all data transfers via <u>all</u> resident devices," and thus the claims do not require that all types of network connections be disabled. ECF No. 271-2 at 37; *see also* Hearing Tr. at 95 (CUPP arguing at the summary judgment hearing that Trend Micro's product infringes because it "shuts down all data transfers for *some* means of communications" (emphasis added)). However, "claims are interpreted with an eye toward giving effect to all terms in the claim." *Bicon, Inc. v. Straumann Co*., 441 F.3d 945, 950 (Fed. Cir. 2006). CUPP's position is contrary to the plain meaning of the claim, because by arguing that some data transfer may still take place, CUPP subverts the requirement that "all"—*i.e.*, 100%—data transfer be disabled. *See, e.g., Depomed, Inc. v. Purdue Pharma L.P*., 2017 WL 1319818, *20 (D.N.J. 2017) (construing term "all" in "until all of said drug is released" to mean 100% of the drug); *see also Cent. Admixture Pharmacy Servs., Inc. v. Advanced Cardiac Sols., P.C*., 482 F.3d 1347, 1355 (Fed. Cir. 2007) ("Claims mean precisely what they say.").

Moreover, the claims do, in fact, state that all data transfers are disabled; specifically, all of those data transfers that occur "via resident devices resident on the mobile device." The addition of that qualifier does not change the regular meaning of "all," but rather, defines the scope of data transfers that must be disabled. Therefore, the claim language does not indicate that this limitation may be satisfied by disabling all data transfers via "at least one" or "a" resident device, but instead, all data transfer via resident devices that reside on the mobile device. CUPP's interpretation fails to give meaning to the "via resident devices *resident on the mobile device*" language.

Trend Micro's position is further supported by the specification. The '462 and '421 patents are in the network security family of patents, and share the same specification. The specification contains one reference to "data transfer," in a description of an embodiment in which "a mobile device 310 attempts to connect to the internet 330 without the mobile security system 345 band not from within the trusted enterprise 340, all data transfer connections including LAN connection, USB-net, modem, Bluetooth, WiFi, etc. may be closed." *See, e.g.*, '462 patent, at 9:54–60. In this embodiment, "[t]he mobile device 310 may be totally isolated and unable to connect to any network, including the internet 330." *Id.* The sole description in the specification of data transfer being disabled is thus contrary to CUPP's interpretation of the claim language, which would permit the mobile device to continue to receive data transfer even when not connected to a secure network or coupled to a trusted security device.

In its response brief, CUPP argues that a "feature lock" in the Mobile Security products satisfies the limitations requiring "disabling all data transfer via resident devices resident on the mobile device" in claim 11 of the '462 patent and claim 1 of the '421 patent. However, Trend Micro urges that this theory was not disclosed in Dr. Mitzenmacher's report, and thus should not be considered. The Court agrees. CUPP cites ¶¶ 229–30, 397, 399, 403–04, and 411–12 of Dr. Mitzenmacher's report for support, but these references either do not refer to the "lock" feature or "locking" in the context of satisfying this claim element, or do not explain that the lock feature disables *all* data transfer. ECF No. 271-2 at 27. For example, ¶ 399 cites a reference that describes setting a policy "to completely lockdown systems to only the applications that your organization wants"; however, restricting access to applications except for those approved by an organization is not the same as blocking all data transfer. Similarly, ¶¶ 397, 403, and 411 describe using the feature lock policy to assess "access points," and whether those access points are allowed, but do not explain what access points are nor how they relate to the particular claim elements at issue. In addition, most of these paragraphs reference feature locking in string cites, without explanation or indication that Dr. Mitzenmacher is expressly relying on the feature lock element to satisfy the claim limitation. CUPP's new feature lock argument was not fully disclosed in Dr. Mitzenmacher's report, and accordingly, the Court will not consider it.

For the foregoing reasons, the Court concludes that the language for disabling "all data transfer via resident devices resident on the mobile device" in claim 11 of the '462 patent and claim 1 of the ’421 patent means the mobile device cannot transfer any data via any resident device resident on the mobile device. Because CUPP has not demonstrated that all modes of transferring data on the mobile device are disabled for the products accused of infringing these claims, summary judgment of non-infringement is appropriate.

e. Non-infringement based on no evidence of direct infringement of claim 11 of the ’444 patent and claim 11 of the ’462 patent

Trend Micro moves for summary judgment of non-infringement of claim 11 of the ’444 patent and claim 11 of the ’462 patent,[7] on the grounds that there is no evidence that these method claims were directly infringed in the United States.

Because claim 11 of the ’444 patent and claim 11 of the ’462 patent are both method claims, to show direct infringement, CUPP must show that Trend Micro has practiced each step of the asserted methods in the United States. *See Meyer Intell. Props. Ltd. v. Bodum, Inc.*, 690 F.3d 1354, 1371 (Fed. Cir. 2012).

Trend Micro argues that summary judgment of non-infringement is appropriate because Dr. Mitzenmacher has not shown that Trend Micro used any accused product in the United States in the particular manner he relies on to show infringement, *i.e.*, with the same combination of settings in Trend Micro’s Mobile Security product. For example, for claim 11 of the ’444 patent, Dr. Mitzenmacher’s infringement theory recites using the Mobile Security product in conjunction with the MARS service, but provides no evidence that Trend Micro or a Trend Micro employee has ever used Mobile Security in the United States in conjunction with MARS. Trend Micro further argues that it develops its products primarily in Asia, and thus it is not a foregone conclusion that any testing or development occurs in the United States. *E.g.*, Pltf. Opp.

[7] The Court notes that it has already granted summary judgment of non-infringement of claim 11 of the ’462 patent, and therefore, this argument is moot as to this claim.

App. 387 (testimony of Trend Micro employee, noting that MARS was "mainly developed in the R&D center in China").

CUPP responds by pointing to deposition testimony of Trend Micro employees as proof that the accused products were tested by Trend Micro in an infringing manner in the United States. *See* ECF No. 271-2 at 40–41 (citing Pltf. Opp. App. 372–73, 388; Def. App. 6117, Cole Rep. ¶ 125). In addition, CUPP argues that Trend Micro does not address its alternative theory of joint infringement, namely that Trend Micro directly infringes the asserted patents through joint infringement with Trend Micro customers. CUPP also argues that sale of a product that is capable of performing a patented method qualifies as direct infringement, citing *Quanta Computer, Inc. v. LG Elecs, Inc.*, 553 U.S. 617 (2008).

The Supreme Court in *Quanta* held that sale of a product capable of performing a patented method could be used to evaluate patent exhaustion, but did not decide whether sale of a product capable of performing a patented method counts as a "sale" for purposes of direct infringement under 35 U.S.C. § 271. *Id.* at 629–30. CUPP effectively asks this Court to disregard post-*Quanta* Federal Circuit case law, which makes clear that, for method claims, "[d]irect infringement *only* occurs when someone performs the claimed method." *Lucent Techs., Inc. v. Gateway, Inc.*, 580 F.3d 1301, 1317 (Fed. Cir. 2009) (emphasis added); *see also Ericsson, Inc. v. D-Link Sys., Inc.*, 773 F.3d 1201 (Fed. Cir. 2014) ("[O]ur decision in *SiRF* did not create direct infringement liability whenever an alleged infringer sells a product that is capable of executing the infringing method.").

Regarding the evidence cited by CUPP, the Court finds that the employee testimony does, albeit weakly, create a fact question as to whether Trend Micro performed the claimed method in the United States. Mr. Park, a Trend Micro employee, testified that although he did not know whether Trend Micro used Mobile Security for Enterprise for its own employees, he did install Mobile Security on his phone. Def. App. 6117. Specifically, he testified he "installed it when [he] was a product manager to test – to use the feature, to test the features, but it was not deployed by the company." *Id.* He further testified that he was not aware of any other Trend Micro employees who installed it on their phones. *Id.* When asked whether any Trend Micro personnel in the United States participated in any testing of MARS, Trend Micro employee Mr. Zhang responded, "[i]f there was any then probably they would perform drills in terms of emulating when the network was down and what was happening. So if there was any, like I said, probably drills of that kind." Pltf. Opp. App. 387–88.

At this juncture, the Court denies summary judgment on this issue, finding that the testimony of Trend Micro employees relied on by CUPP creates a fact question as to whether Trend Micro used the accused products, namely Mobile Security in conjunction with the MARS server, in an infringing way in the United States, thereby supporting a jury question as to infringement of claim 11 of the '444 patent. However, the Court notes the relative weakness of CUPP's evidence, such that it may be appropriate for the Court to revisit the issue after CUPP's presentation of evidence. The Court does not reach the question of joint infringement.

f. Invalidity of claim 11 of the '202 patent based on lack of written description

Trend Micro moves for summary judgment that claim 11 of the '202 patent is invalid for lack of written description. Compliance with the written description requirement under 35 U.S.C. § 112 is a question of fact, which is assessed on a per-claim basis. In determining whether the written description requirement is met, the Court considers "whether the disclosure of the application relied upon reasonably conveys to those skilled in the art that the inventor had possession of the claimed subject matter as of the filing date." *Ariad Pharm., Inc. v. Eli Lilly &*

Co., 598 F.3d 1336, 1351 (Fed. Cir. 2010) (en banc). "The written description requirement is not met if the specification merely describes a 'desired result.'" *Vasudevan Software, Inc. v. MicroStrategy, Inc.*, 782 F.3d 671, 682 (Fed. Cir. 2015).

Trend Micro argues that the "controller" element, as described in claim 11, lacks written description support. Claim 11 claims a removable media device comprising, in part:

> a controller configured to intercept a request for the data, determine whether to allow the request for the data based on a security policy, the security policy implementing content analysis and risk assessment algorithms, and provide requested data based on the determination.

'202 patent, cl.11.

Thus, claim 11 describes a controller configured to perform three tasks: (i) intercept a request for data, (ii) determine whether to allow the request based on a security policy, and (iii) provide requested data based on that determination. Further, the controller decides whether to allow the request "based on a security policy," which implements content analysis and risk assessment algorithms.

Trend Micro contends that the "controller" element of claim 11 lacks written description support because the specification only describes the controller generically, without any instruction or guidance as to how the controller actually performs these claimed tasks. CUPP responds that the claim language does not require that the controller itself perform the recited tasks; instead, the claim provides that the security policy implements the content analysis and risk assessment algorithms, which the specification describes as being performed by the security engine, the security device, and the redirection module.

After reviewing the specification, the Court agrees with Trend Micro that the controller is only described generically, without any discussion of how the controller itself is to "intercept" a data request, "determine" whether to allow it, and if allowed, "provide" the data requested. The specification describes the controller generally as existing on a USB flash drive.[8] Although the specification describes the controller being able to control access to the flash memory stored on that USB drive, it is only described as doing so via a password; there is no discussion or description of the controller implementing content analysis or risk assessment algorithms to assess a request for data. *See* '202 patent, at 19:3–6. This is in contrast to extensive discussion in the specification of other components—namely, the security engine, the security device, and the redirection module, all of which are described with detail in the specification as performing content analysis and risk algorithm assessment.[9] For example, the specification describes how a "security engine" operates, including the subcomponents it may use to perform content analysis and risk assessment algorithms.[10] Given the detail in the disclosure about how other components perform the analysis, the paucity of information about how a controller on a flash drive would perform the same functions indicates that the inventor may not have had possession of this

[8] *See* '202 patent, at 17:66–67 ("The non-secured USB flash drive 1704 includes a controller 1714 and flash memory 1716."); *id.* at 18:18–20 ("The non-secured USB flash drive 1704 is any thumb drive that contains a controller 1714 and flash memory 1716. The controller 1714 is a flash controller."); *id.* at 18:48–50 ("The secured USB flash drive 1804 includes a controller 1814 and flash memory 1816."); *id.* at 18:55–57 ("The secured USB flash drive 1804 is any thumb drive with at least some security that contains a controller 1814 and flash memory 1816."); *id.* at 19:3–6 ("Upon entering a correct password, the controller 1814 may allow access to the data stored in the flash memory 1816 and/or decrypt data from the flash memory 1816."); *id.* at 19:38–40 ("The removable media device 1904 may comprise the controller 1916, the flash memory 1918, and the login module 1920."); *id.* at 19:42–43 ("The controller 1916 may be any controller that controls access to the flash memory 1918.").

[9] For example: '202 patent, at 8:25–34 ("To provide a higher security level provided by antivirus and antispyware software, the security engines 530 on each mobile security system 345 may implement content analysis and risk assessment algorithms. Operating for example at OSI Layer 7 and above (mobile code encapsulated within Layer 7), these algorithms may be executed by dedicated High Risk Content Filtering (HRCF) that can be controlled by a rules engine and rule updates. The HRCF will be based on a powerful detection library that can perform deep content analysis to verify real content types. . . ."). The specification goes into detail as to how this risk assessment could occur. *Id.* at 16:14–19 ("In one embodiment, a security engine 1410 assigns a weight and rank for every transfer object based on its type, complexity, richness in abilities, source, etc. The Security engine 1410 may assign weight based on the Source using a list of known dangerous or known safe sources.").

[10] *E.g.*, '202 patent, at 8:12–24 ("The security engines 530 execute security programs based on the security policies 535 and on security data 540, both of which may be developed by IT managers. Security engines 530 may include firewalls, VPN, IPS/IDS, antivirus, antispy ware, malicious content filtering, multilayered security monitors, Java and bytecode monitors, etc. Each security engine 530 may have dedicated security policies 535 and security data 540 to indicate which procedures, content, URLs, system calls, etc. the engines 530 may or may not allow. The security engines 530, security policies 535 and security data 540 may be the same as, a subset of, and/or developed from the engines, policies and data on the network security system 320.").

particular claimed invention—a controller on a USB flash drive capable of determining whether to allow a request for data based on a security policy implementing content analysis and risk assessment algorithms—as of the filing date.

In addition, the Court finds that the report of CUPP's validity expert for the '202 patent, Dr. Jaeger, is not sufficient to raise a genuine issue of material fact as to whether there is adequate written description for claim 11 of the '202 patent. *See* Hearing Tr. at 63–64. In ¶ 265 of his report, Dr. Jaeger points to a portion of the specification discussing the security engine's ability to scan data, and opines that "a POSITA would understand that this security functionality is not limited to be only on the computer, but may be located as part of the controller because the controller provides the access to the data and that prior to getting access to that data, it may be [sic] have its contents analyzed and perform a risk assessment." Pltf. App. (ECF No. 241-26) 642 (quoting '202 patent, at 24:54–61). Dr. Jaeger also points to a portion of the specification explaining that variations of the embodiments described therein are exemplary and limited only by the claims, and explains that "[a] POSITA would understand by reading that paragraph of the specification that the controller could include security policies as described in the specification." *Id.* at 643 (quoting '202 patent, at 27:13–32). The Court finds that neither of these opinions offered by Dr. Jaeger demonstrate or explain how the written description actually or inherently discloses the controller determining whether to allow a request for data based on a security policy implementing content analysis and risk assessment algorithms. *See TurboCare Div. of Demag Delaval Turbomachinery Corp. v. Gen. Elec. Co.*, 264 F.3d 1111, 1118–20 (Fed. Cir. 2001) (to comply with the written description requirement, the claim limitation must be actually or inherently disclosed; that the limitation may be obvious from the disclosure is not enough); *Tronzo v. Biomet, Inc.*, 156 F.3d 1154, 1159 (Fed. Cir. 1998) ("In order for a disclosure to be inherent, however, the missing descriptive matter must necessarily be present in the . . . specification such that one skilled in the art would recognize such a disclosure.”). Nor do the portions of the ’202 patent cited by Dr. Jaeger refer to the controller making the claimed determination.

In response, CUPP argues that the controller is capable of performing the claimed functions, but the claim does not require it to do so. Hearing Tr. at 9–10. Specifically, CUPP argues that the specification “does not limit the component onto which the operation is performed” and that due to the claim’s “based on” language—*i.e.*, that the controller is configured to “determine whether to allow the request for the data *based on* a security policy”—the controller does not have to perform the recited functions itself. *See* ECF No. 271-2 at 18. CUPP further maintains that the security policy need not be located on the controller and the claimed operations can be performed on the other components for which it is undisputed there is written support in the specification. *Id.* at 19 (arguing “the controller can call another component to access the security policy that uses the content analysis and risk assessment algorithms”).

The Court disagrees. As discussed, the specification contains no written description of the controller performing the claimed “determine” function, based on a security policy implementing content analysis and risk assessment algorithms. CUPP’s alternate position—that there is no requirement for the controller to do the actual analysis, and other components can perform the claimed function—relies on a tortured reading of the claim language such that the controller does not perform the functions that are clearly assigned to it. Claim 11 expressly states that the controller is configured to “determine whether to allow the request for the data based on a security policy”; the claim language does not contemplate or explain how the controller could rely on or apply the results of another component performing that determination.

Had the patentee intended the claim scope to encompass other components besides the controller performing the "determine" function, the claim language could have provided so explicitly. In addition, even if the language could be read to allow for the "determine" step to be performed elsewhere by other components, the specification contains no support for how the controller is to implement those results to satisfy the claim limitation. Put differently, if some component besides the controller performs the content analysis or risk assessment algorithms, it is unclear what else the controller does to satisfy the claim requirement that it "determine whether to allow the request for the data based on a security policy," let alone whether there is support in the written description for the controller performing such a function.

For the foregoing reasons, the Court concludes that no reasonable fact finder could find that the written description requirement is satisfied for claim 11 of the '202 patent. The Court grants summary judgment to Trend Micro on the issue of validity of claim 11 of the '202 patent.

g. Pre-suit indirect or willful infringement

Trend Micro moves for summary judgment of no pre-suit indirect or willful infringement, arguing that it had no pre-suit knowledge of the asserted patents. In response, CUPP represents that it is not asserting willful infringement for the '202 and '444 patents, and is not seeking pre-suit damages for indirect infringement. Therefore, the only patents for which pre-suit knowledge is relevant are the asserted *CUPP2* patents—*i.e.*, the '400, '462, '421, and '834 patents—which form the basis of CUPP's remaining claims for willful infringement.

"To willfully infringe a patent, the patent must exist and one must have knowledge of it." *State Indus., Inc. v. A.O. Smith Corp.*, 751 F.2d 1226, 1236 (Fed. Cir. 1985). CUPP argues that Trend Micro had pre-suit knowledge of the *CUPP2* patents because of the earlier-filed *CUPP1* lawsuit and *CUPP1* patents, some of which share the same inventor as, or are related to, the *CUPP2* patents. CUPP also argues that Trend Micro filed several IPR petitions against *CUPP1* patents, and in preparing those petitions, Trend Micro "had to have thoroughly investigated CUPP's patent portfolio." ECF No. 271-2 at 45. In the alternative, CUPP argues that Trend Micro was deliberately indifferent to the existence of the *CUPP2* patents, and that deliberate indifference can substitute for actual knowledge.

The Court finds that the fact that CUPP asserted the *CUPP1* patents against Trend Micro, without more, is insufficient to create a genuine issue of material fact as to whether Trend Micro had pre-suit knowledge of the *CUPP2* patents. At oral argument, CUPP conceded that, other than the fact that it filed the *CUPP1* complaint against Trend Micro in 2018, it has no evidence that Trend Micro knew of the asserted *CUPP2* patents prior to the *CUPP2* complaint being filed in 2020. Hearing Tr. at 11. For instance, CUPP points to no evidence that any individual at Trend Micro reviewed the *CUPP2* patents or were otherwise actually aware of them. Nor does CUPP point to any pre-suit notice it provided to Trend Micro of the *CUPP2* patents.

Instead, CUPP relies solely on attorney argument to connect the dots, arguing that Trend Micro had actual pre-suit knowledge of the asserted *CUPP2* patents because: the parents to the '400, '462, and '421 patents were asserted in *CUPP1*; the '400, '462, and '421 patents share a common inventor with patents asserted in *CUPP1*; the asserted *CUPP2* patents involve subject matter related to the patents asserted in *CUPP1*; as a sophisticated company, Trend Micro should have been aware of CUPP's patent portfolio after *CUPP1* was filed; and "based on standard due diligence," Trend Micro would have been aware of patents related to the *CUPP1* patents challenged at IPR, including certain asserted *CUPP2* patents. *See* ECF No. 271-2 at 45–46.

However, CUPP does not point to any authority from the Federal Circuit for the proposition that actual knowledge of a patentee's entire portfolio can be imputed to a would-be infringer simply because the patentee asserts related patents in a different lawsuit. In fact, district courts routinely hold the opposite, recognizing that "[k]nowledge of a patent portfolio generally is not the same thing as knowledge of a specific patent." *Finjan, Inc. v. Cisco Sys. Inc*., No. 17-CV-00072-BLF, 2017 WL 2462423, at *5 (N.D. Cal. June 7, 2017); *see also Intell. Ventures II LLC v. Sprint Spectrum, L.P.*, No. 217CV00662JRGRSP, 2019 WL 1987172, at *2 (E.D. Tex. Apr. 12, 2019) ("[K]nowledge of other patents in the same portfolios, with some of those being within the same family as the asserted patents, [is] insufficient to defeat a motion for summary judgment for pre-suit willfulness."), *report and recommendation adopted*, No. 217CV00661JRGRSP, 2019 WL 1979866 (E.D. Tex. May 3, 2019). In addition, CUPP acknowledged that none of the *CUPP2* patents were cited in any of the IPR proceedings filed by Trend Micro challenging the *CUPP1* patents, and moreover, some of the *CUPP2* patents had not even issued yet when those IPR petitions were filed. Hearing Tr. at 12; ECF No. 271-2 at 46 (noting that the '400 patent issued in September 2019, after the IPR petition for the '202 patent was filed on March 8, 2019). Given the lack of contrary guidance from the Federal Circuit or any actual evidence of Trend Micro's knowledge of CUPP's portfolio when it filed the IPRs, the Court agrees that "simply pointing out knowledge of the parent of one of the asserted patents or knowledge of other patents that share the same inventor as one of the asserted patents is insufficient" to create a fact question as to actual knowledge. *Intell. Ventures II LLC*, 2019 WL 1987172, at *2.

In addition, even if the Court assumes, without deciding, that willful blindness or deliberate indifference can substitute for actual knowledge of the *CUPP2* patents in the willfulness inquiry,[11] CUPP has not shown any evidence that Trend Micro was, in fact, willfully

[11] CUPP cites only *SEB S.A. v. Montgomery Ward & Co.*, 594 F.3d 1360, 1375–76 (Fed. Cir. 2010), to argue that deliberate indifference can substitute for actual knowledge in the willful infringement inquiry; however, this case addresses the "deliberate indifference" standard in the context of induced infringement, not willful infringement. However, the Court notes that several courts have extended the Supreme Court's reasoning regarding willful blindness

blind to the existence of the asserted *CUPP2* patents prior to suit. Willful blindness has two requirements: "(1) the defendant must subjectively believe that there is as high probability that a fact exists and (2) the defendant must take deliberate actions to avoid learning of a fact." *Global–Tech Appliances, Inc. v. SEB S.A.*, 563 U.S. 754, 769 (2011). Plaintiff puts forth no specific evidence in support of either requirement, and thus has not established a fact question as to willful blindness.

For the foregoing reasons, the Court finds that there is no evidence that Trend Micro had pre-suit knowledge of the '400, '462, '421, and '834 patents. As a result, Trend Micro is entitled to summary judgment on CUPP's claims of pre-suit indirect and willful infringement.

h. Indirect infringement

Trend Micro moves for summary judgment on CUPP's claims of indirect infringement against Trend Micro, arguing that CUPP has not established any underlying direct infringement by Trend Micro's customers.

Proof of indirect infringement, *i.e.* contributory or induced infringement, requires proof of underlying direct infringement. *Limelight Networks, Inc. v. Akamai Techs., Inc.*, 572 U.S. 915, 921 & n.3 (2014). Trend Micro argues that CUPP puts forth no evidence of direct infringement by Trend Micro's customers, and instead relies solely on the expert opinions of Dr. Cole and Dr. Mitzenmacher describing how the accused products may be used by customers in an infringing way. According to Trend Micro, this is insufficient to establish direct infringement by Trend Micro's customers, warranting summary judgment against CUPP's claim that Trend Micro indirectly infringes the asserted claims. ECF No. 229-1 at 4 (citing *Fujitsu Ltd. v. Netgear*

in the induced infringement context in *Global-Tech Appliances, Inc. v. SEB S.A.*, 563 U.S. 754 (2011), to conclude that a finding of willful blindness can, in effect, satisfy the knowledge requirement when proving willful infringement. *See, e.g.*, *Corephotonics, Ltd. v. Apple, Inc.*, 2018 WL 4772340, *9–10 (N.D. Cal. 2018).

Inc., 620 F.3d 1321, 1329 (Fed. Cir. 2010) (where "manuals and expert testing only show that the products are capable of infringing, they do not provide evidence of direct infringement")).

The Court disagrees. The Federal Circuit has recognized that "where an alleged infringer designs a product for use in an infringing way and instructs users to use the product in an infringing way, there is sufficient evidence for a jury to find direct infringement." *Toshiba Corp. v. Imation Corp.*, 681 F.3d 1358, 1365 (Fed. Cir. 2012) ("Appellees designed the DVDs to be used in an infringing way and instructed users to use them in the infringing way by finalizing the DVDs or using the disc-at-once mode. This is sufficient to preclude summary judgment."). Here, both Dr. Mitzenmacher and Dr. Cole describe how the accused products are installed and operated, and point to evidence showing that Trend Micro knowingly distributes materials "encouraging its customers and users to install and operate the Accused Products" in an infringing way. *See, e.g.*, Mitzenmacher Rep. ¶ 3650; Cole Rep. ¶ 3802.

Direct infringement can be shown by circumstantial evidence. *Toshiba*, 681 F.3d at 1364 ("Circumstantial evidence must show that at least one person directly infringed an asserted claim during the relevant time period."). CUPP need not produce an actual Trend Micro customer using the accused products in an infringing way to create a triable issue of material fact of direct infringement by Trend Micro's customers. The Court finds that summary judgment is inappropriate on CUPP's claims of indirect infringement on these grounds.

IV. CUPP's Motion for Partial Summary Judgment

CUPP seeks summary judgment of validity as to the '202 patent,[12] arguing that Trend Micro waived the right to assert obviousness and that Trend Micro's proposed modifications would render the prior art inoperable, and that claim 11 of the '202 patent is not invalid for lack

[12] CUPP also argues that Trend Micro waived the right to assert obviousness as to the '079 and '272 patents, which the Court does not reach because the case is stayed as to all asserted claims of the '272 and '079 patents.

of written description. CUPP also moves for summary judgment of infringement as to claim 11 of the ’202 patent, and summary judgment of validity as to the ’834 patent.

As discussed above, this Court grants summary judgment to Trend Micro that claim 11 of the ’202 patent is invalid for lack of written description, so CUPP’s request for summary judgment of validity on that point is denied. The Court addresses the remainder of CUPP’s arguments regarding the ’202 patent below.

a. Validity of the ’202 patent

i. Waiver

CUPP seeks summary judgment of validity and non-obviousness for the ’202 patent, on the grounds that Trend Micro waived the right to assert obviousness for this patent by filing an IPR petition challenging its validity. CUPP’s argument is based on a common law theory of waiver; CUPP cites Fifth Circuit law on waiver to argue that Trend Micro intentionally relinquished the right to challenge obviousness in the district court when it filed its IPR petitions, but provides no patent case authority in which a defendant was deemed to have generally waived raising obviousness by filling an IPR.

Congress has explained how the filing of an IPR impacts district court litigation by enacting IPR estoppel in 35 U.S.C. § 315(e), which does not apply here. Under § 315(e), if an accused infringer files an IPR, it is subsequently estopped from asserting invalidity in the district court “on any ground that . . . [was] raised or reasonably could have [been] raised” in the IPR. However, because IPRs are limited to prior art patents and publications, a defendant could not raise a prior art product or system in an IPR, and thus is not estopped from asserting such prior art to argue invalidity in the district court. Had Congress intended to prevent all invalidity challenges in the district court after the filing of an IPR petition, it could have expanded the scope of § 315(e) accordingly. Here, because Trend Micro's district court obviousness theories are based on prior art products—the SonicWall and ClipDrive Bio—Trend Micro is not estopped from asserting invalidity on those grounds.

Even if CUPP had authority supporting its position that, in addition to statutory estoppel under § 315(e), common law waiver could potentially apply, CUPP has not shown that it is appropriate here. In the Fifth Circuit, the elements of waiver include an existing right held by a party, the party's knowledge of its existence, and the party's actual intent to relinquish the right, or intentional conduct inconsistent with the right. *Thompson v. Bank of Am. Nat. Ass'n*, 783 F.3d 1022, 1025 (5th Cir. 2015). CUPP has not established that, by filing an IPR petition challenging the '202 patent, Trend Micro expressed actual intent to relinquish its right to challenge obviousness in this Court with prior art products or systems. *See id.* ("Where waiver is claimed by inference rather than express renunciation, 'it is the burden of the party who is to benefit . . . to produce conclusive evidence that the opposite party unequivocally manifested its intent to no longer assert its claim.'"). Trend Micro points to the fact that, even after filing the IPRs, it included the Sonic Wall and ClipDrive Bio products in its invalidity contentions, conducted discovery on those products, and included them in its expert reports on invalidity. In addition, given that Trend Micro was not permitted to assert prior art products before the PTAB, it is not clear how filing an IPR can reflect an intentional abandonment of the right to assert those pieces of prior art in this Court. CUPP's Motion for Partial Summary Judgment on this point is denied.

ii. Obviousness

CUPP moves for summary judgment of validity and non-obviousness for claim 21 of the '202 patent, arguing that, as part of the obviousness analysis, Trend Micro's expert invalidity expert for the '202 and '400 patents, Dr. Meldal, proposes modifying the ClipDrive Bio prior art product in a way that would render it inoperable. CUPP cites caselaw indicating that if a proposed combination or modification of a prior art system would render it inoperable, that inoperability would "teach away" from the combination and cannot be the basis for an obviousness theory. *E.g.*, *In re Gordon*, 733 F.2d 900, 902 (Fed. Cir. 1984) ("The mere fact that the prior art could be so modified would not have made the modification obvious unless the prior art suggested the desirability of the modification. . . . [I]f the French apparatus were turned upside down, it would be rendered inoperable for its intended purpose. . . . In effect, French teaches away from the . . . proposed modification.").

Claim 21 of the '202 patent describes, in part, "injecting redirection code into the digital device after detecting the removable media device is coupled to the digital device, the redirection code configured to intercept a first function call and configured to execute a second function call in place of the first function call." For this element, Dr. Meldal opines that the prior art ClipDrive Bio USB flash drive device could be modified to "inject redirection code" by sending a SSDADM.sys file (the redirection code) from the ClipDrive Bio to the computer. Pltf. App. 547–64 (ECF No. 241-23) ("Meldal Rep.") ¶¶ 117–18; *see also id.* ¶¶ 69, 77–80. However, CUPP contends that SSDADM.sys is a driver file that must be present on the computer for the ClipDrive Bio to communicate with the computer, and thus without it already present on the computer, nothing would happen when ClipDrive Bio is inserted. ECF No. 242-2 at 26–27. As a result, CUPP maintains that Trend Micro's theory based on ClipDrive Bio is inoperable, and thus cannot be the basis of an obviousness argument.

In response, Trend Micro points other portions of Dr. Meldal's report, in which he describes a technique based on the prior art reference *Yan* to facilitate the injection of SSDADM.sys into the digital device from ClipDrive Bio, which does not depend on

SSDADM.sys already being present on the digital device. *See* Meldal Rep. ¶¶ 77–80. Specifically, Trend Micro points to a paragraph in Dr. Meldal's report that states it would be obvious to a POSITA to inject the SSDADM.sys module onto the digital device, and one method of doing so would be by including "the DLLs described above used for DLL replacement to intercept a first function call" and then following the method "described in, for example, Yan at ¶¶ 32–35 and Figure 2." *Id.* ¶ 77; *see also* ECF No. 256-1 at 18 n.6 ("A Dynamic Linked Library (DLL) is a collection of code."). *Yan* describes how when a secure memory device is connected to a host device, "software libraries for operating the secure memory device are loaded and installed onto the host device," without reference to SSDADM.sys. Def. App. 476 (ECF No. 256-5) ¶ 32. Thus, Trend Micro contends that CUPP ignores this proposed modification of the ClipDrive Bio by *Yan*, which according to Dr. Meldal, would render the ClipDrive Bio operable despite the concerns identified by CUPP.

In sum, CUPP posits that the modification of the ClipDrive Bio, as proposed by Trend Micro in support of its obviousness theory, is inoperable, warranting summary judgment of validity. In response, Trend Micro points to evidence, namely Dr. Meldal's opinion, to support its position that ClipDrive Bio, as modified by *Yan*, would still be operable when used in the manner proposed by Trend Micro. In light of the foregoing, the Court finds that there is a fact question as to whether Trend Micro's proposed modification of ClipDrive Bio, in light of *Yan*, would be inoperable. The Court declines to grant summary judgment of non-obviousness for claim 21 of the '202 patent at this time.

a. Infringement of claim 11 of the '202 patent

CUPP seeks summary judgment of infringement of claim 11 of the '202 patent, arguing that Trend Micro's Portable Security product, a USB flash drive, contains all four elements of claim 11 of the ’202 patent. In response, Trend Micro argues that CUPP has not shown two elements of claim 11, the “login engine” element and the “controller” element.

As to the “login engine” element, claim 11 of the ’202 patent recites:

> a login engine configured to detect coupling to a digital device, the login engine further configured to inject redirection code into the digital device after detecting the coupling to the digital device, the redirection code being configured to intercept a first function call and configured to execute a second function call in place of the first function call;

’202 patent, cl.11.

To satisfy this element, CUPP points to the “Scanning Tool” contained in the Portable Security flash drive product, which detects when the flash drive is inserted into a computer. ECF No. 242-2 at 34 (citing Cole Rep. ¶ 1876). CUPP further argues that this Scanning Tool “injects redirection code” into the PC once inserted, using a “LaunchClient” function, which creates a temporary folder on the computer to store “necessary files needed by TMPSCore.exe and ScanTool.exe,” the tools Portable Security uses for scanning. *Id.* (citing Cole Rep. ¶¶ 1871, 1876). For the “intercept a first function call” and “execute a second function call in place of the first function call” elements, CUPP points to Dr. Cole’s opinion that Portable Security intercepts read and write attempts to the USB and then determines whether those attempts should be permitted, using the HouseCall core module and Behavior Monitor Core Driver. *Id.* at 35–36 (citing Cole Rep. ¶¶ 1871, 1883). Dr. Cole further opines that the HouseCall module intercepts function calls from threats known as “rootkits.” *Id.*

In response, Trend Micro argues, *inter alia*, that CUPP has not shown that because the read/write requests to the USB are directed to the USB itself, Portable Security does not “intercept” a function call that would otherwise have a different destination, relying on its non-infringement expert, Dr. Black. *See* Pltf. App. 707 ¶¶ 18–20 (citing Pltf. App. 474 (“Any request to read or write data stored on the Portable Security flash memory received by the controller would be directed to the controller in the first place, and therefore would not be an interception.”)). In reaching that conclusion, Dr. Black relies on a conversation with a Trend Micro employee, William Chang. *Id.* at 747. Moreover, Trend Micro contends that CUPP cannot point to rootkits to satisfy the “intercept a first function call” limitation, arguing that rootkits do not qualify as function calls and are unrelated to attempts to read/write to the USB.

In light of the foregoing, the Court concludes that a reasonable jury could find that the Portable Security product does not satisfy the “login engine” limitation of claim 11 of the ’202 patent. CUPP has not shown the absence of a genuine issue of material fact as to whether the Portable Security product infringes claim 11 of the ’202 patent, and thus summary judgment is not appropriate.

b. Validity of the ’834 patent

CUPP moves for summary judgment of validity of claim 1 of the ’834 patent, arguing that Trend Micro’s theory of obviousness is insufficient because Trend Micro’s invalidity expert, Dr. Franz, did not sufficiently identify the “confidentiality level” and “integrity level” claim elements in the prior art.

Claim 1 of the ’834 patent recites a confidentiality level and an integrity level, which are used in conjunction with one or more virtual machines to associate particular datasets with a virtual machine that has corresponding confidentiality and integrity levels. This Court previously construed “integrity level” as “a security aspect, separate from the confidentiality level, that indicates reliability.” ECF No. 151 at 23.

Dr. Franz opines in his report that claim 1 of the ’834 patent is invalid as obvious in light of the *Focke* reference. *See* Pltf. App. 609–16 (ECF No. 241-25) (“Franz Rep.”) ¶ 31. CUPP argues that in providing his theory of obviousness as to claim 1 of the ‘834 patent, Dr. Franz did not sufficiently identify specific parameters in the prior art that correspond to the confidentiality and integrity levels, and instead simply makes vague references to papers incorporated by reference. Specifically, CUPP contends that Dr. Franz does not identify what in the *Focke* reference corresponds to the confidentiality level, but instead makes vague reference to the "Bell-LaPadula paper" (which *Focke* incorporates by reference), and the "security level" described within that paper. Similarly, for the integrity level, CUPP argues that Dr. Franz only references the Biba paper (which *Focke* incorporates) without identifying a specific parameter, and have not shown that the integrity level described in Dr. Franz's report corresponds to "reliability," as required by the Court's construction.

The Court disagrees. A review of Dr. Franz's report shows that he identifies the "confidentiality" and "integrity" levels with sufficient clarity such that summary judgment is inappropriate on these grounds. Specifically, in his report, Dr. Franz identifies the portions of Bella-LaPadula and Biba, incorporated into *Focke* by reference, upon which he relies to reach his obviousness conclusions. *See Zenon Env't, Inc. v. U.S. Filter Corp*., 506 F.3d 1370, 1378 (Fed. Cir. 2007) ("Incorporation by reference '. . . makes clear that the material is effectively part of the host document as if it were explicitly contained therein.'").

For example, as to the confidentiality level, Dr. Franz describes how Bell-LaPadula "describes a model to ensure the confidentiality of information, i.e., restrict access to information only to uses (or processes, etc.) who have the necessary clearance to see it." Pltf. App. 617–38 (ECF No. 241-25) ("Franz Rep. App'x") ¶ 43.[13] He explains that *Focke* refers to the Bell-LaPadula confidentiality level as a "security level," and opines that a POSITA would understand

[13] In explaining why claim 1 of the '834 patent is obvious in light of *Focke*, Dr. Franz incorporates his theory of invalidity as to claims 1 and 13 of the '975 patent, which was previously asserted by CUPP. *See* Franz Rep. ¶¶ 35–66; *see generally* Franz Rep. App'x. The '834 patent is a continuation of the '975 patent and shares the same specification.

the *Focke* security levels are confidentiality levels, in the meaning of the ’834 patent, pointing in part to the Bell-LaPadula model, in which “each ‘process[]’ and program[] in execution’ has a ‘clearance level’ (confidentiality level).” *Id.* ¶¶ 43–46.

Dr. Franz similarly discusses the integrity level element, including an analysis that explains why confidentiality levels are distinguishable from integrity levels, and how the integrity levels from Biba and *Focke* correspond to reliability, as required by the Court’s construction. *See id.* ¶¶ 53–55. Specifically, Dr. Franz explains how Biba describes a model for integrity, in which a database “must ensure that its accuracy is maintained, and modification of the database should be restricted even though it should still be ‘observable to a variety of applications at differing security levels.’” *Id.* ¶ 53. Thus, “[u]nlike confidentiality levels, ‘[i]ntegrity levels . . . are assigned not to prevent information disclosure, [but] to prevent information sabotage.’” *Id.* (all alterations except the first in original). In this way, “[i]ntegrity in Biba (and Focke) therefore is a security aspect that refers to reliability, such as reliability of information . . . [and] therefore are different than, and separate from, the confidentiality levels in Bell-LaPadula (and Focke), as required by the Court’s construction.” *Id.*

In sum, CUPP has not shown that Dr. Franz did not sufficiently identify the “confidentiality level” and “integrity level” claim elements in the prior art. As a result, the Court concludes that summary judgment of non-obviousness as to claim 1 of the ’834 patent is inappropriate on these grounds.

V. Conclusion

For the foregoing reasons, the Court **GRANTS** summary judgment to Trend Micro on CUPP’s claims of infringement of claim 17 of the ’400 patent as to the accused “DLP/DC” products, claim 21 of the ’202 patent, claim 11 of the ’462 patent, and claim 1 of the ’421 patent.

The Court further **GRANTS** summary judgment to Trend Micro that claim 11 of the ’202 patent is invalid for failure to satisfy the written description requirement, and **GRANTS** summary judgment to Trend Micro on CUPP’s claims for pre-suit indirect or willful infringement based on the asserted claims in the ’400, ’462, ’421, and ’834 patents. The remainder of Trend Micro’s Motion for Summary Judgment is **DENIED.** CUPP’s Motion for Partial Summary Judgment is **DENIED** in its entirety.

SO ORDERED.

January 18, 2023.

Barbara M G Lynn
BARBARA M. G. LYNN
UNITED STATES DISTRICT JUDGE